Difference fields and descent in algebraic dynamics, II

Zoé Chatzidakis*(CNRS - Université Paris 7)
Ehud Hrushovski†(The Hebrew University)

Introduction

This second part of the paper strengthens the descent theory described in the first part [4] to rational maps and arbitrary base fields. In particular this is needed in order to obtain the "dynamical Northcott" Theorem 1.11 of Part I in sharp form. As a special case, for $\mathbb{P}^1$ over an algebraically closed field, we recover the theorem of [1].

Stated model-theoretically, our main result is the following:

Theorem 3.2 *Let $(\mathcal{U}, \sigma)$ be an inversive difference field, and $K_1 \subset K_2$ be subfields of the fixed field* $\mathrm{Fix}(\sigma) = \{c \in \mathcal{U} \mid \sigma(c) = c\}$, *with K_2/K_1 regular. Let a, b be tuples in $\mathcal{U}$ such that $SU(a/K_2) < \infty$ and:*

(a) *a belongs to the difference field $K_2(b)_\sigma$ generated by b over K_2;*

(b) *$K_1(b)_\sigma$ is linearly disjoint from K_2 over K_1;*

(c) *$tp(a/K_2)$ is hereditarily orthogonal to* $\mathrm{Fix}(\sigma)$.

Then there is a tuple c in $K_1(b)_\sigma^{\mathrm{perf}}$ such that $a \in K_2(c)_\sigma$ and c is purely inseparable over $K_2(a)_\sigma$. If $tr.deg(K_2(a)_\sigma/K_2) = 1$ and K_1 is perfect, then one can choose c so that $K_1(b)_\sigma \cap K_2(a)_\sigma = K_1(c)_\sigma$.

This result is in fact an easy corollary of a similar statement for *inversive* difference fields, see Proposition 3.1. Stated in the language of the first part [4], the orthogonality condition simply means *fixed-field-free*, but see also section 1 for a more model-theoretic definition. This theorem implies a result which can be stated in geometric terms, given the language of algebraic dynamics (cf. the introduction of [4]):

Theorem 3.3 *Let $K_1 \subset K_2$ be fields, with K_2/K_1 regular, and let $(V_2, \phi_2) \in AD_{K_2}$. Assume that (V_2, ϕ_2) is primitive and that* $\deg(\phi_2) > 1$. *Assume furthermore that for some $n \geq 1$, (V_2, ϕ_2^n) is dominated (in AD_{K_2}) by some object of AD_{K_1}.*

*partially supported by MRTN-CT-2004-512234 and by ANR-06-BLAN-0183
†thanks to the Israel Science Foundation for support, and to the ANR-06-BLAN-0183

(1) *There is some variety* V_3 *defined over* K_1*, and a dominant constructible map* $\phi_3 : V_3 \to V_3$ *also defined over* K_1*, a constructible isomorphism* $h : (V_2, \phi_2) \to (V_3, \phi_3)$*.*

(2) *Assume that the characteristic is* 0*, or that* K_1 *is perfect and* $\dim(V_2) = 1$*. Then* (V_2, ϕ_2) *is rationally isotrivial, i.e., there is some* $(V_3, \phi_3) \in AD_{K_1}$ *which is isomorphic to* (V_2, ϕ_2) *(in* AD_{K_2}*).*

Note that in the general case (1) above, we do not know that (V_3, ϕ_3) can be taken in AD_{K_1}: we only know that ϕ_3 is constructible. The statement of Theorem 3.3 was devised to contain no model-theoretical notions, but the proof will really use only that (V_2, ϕ_2) is fixed-field-free; in fact even this assumption is not needed here, as will be seen in [5] (see point 1 below).

Before describing the organisation of the paper and explaining some of the tools arising in the proof, here are some of the highlights of the third paper [5]. Indeed, Proposition 3.1 and Theorem 3.3 suggest several directions of research.

1. The assumption on $\deg(\phi_2)$ made in Theorem 3.3 is unnecessary:

Theorem. *Let* $K_1 = K_1^{alg} \subset K_2$ *be fields,* $(V_2, \phi_2) \in AD_{K_2}$ *with* V_2 *absolutely irreducible. Assume that* (V_2, ϕ_2) *is dominated by an object of* AD_{K_1}*. Then* (V_2, ϕ_2) *dominates some* $(V_3, \phi_3) \in AD_{K_1}$ *(with* $\dim(V_3) > 0$*). If* (V_2, ϕ_2) *is primitive, it is (constructibly) isotrivial.*

Note the extra assumption of K_1 being algebraically closed. The case not covered by the proof of Proposition 3.1 is when $tp(a/K_1)$ is almost internal to $\mathrm{Fix}(\sigma)$. We use the Galois theory of difference equations (a standard model-theoretic tool, which has to be slightly adapted to our context; see also the end of the introduction of the first part [4]). Assuming K_2 algebraically closed, we show that a is equi-algebraic over K_2 to an element $b \in K_2(a)_{\sigma^{\pm 1}}$ in a translation variety, more precisely satisfying an equation $x \in G \wedge \sigma(x) = x + g$, where G is a (simple) commutative algebraic group and $g \in G(K_2)$. From this the result follows, using the Galois correspondence.

2. The hypothesis of hereditary orthogonality in Proposition 3.1 cannot be removed; see 3.5. However, using a model-theoretic result on canonical bases, one can show that there is some $c \in K_2(a)_{\sigma^{\pm 1}}^{alg}$ such that $tp(a/K_2(c)_{\sigma^{\pm 1}})$ is almost internal to $\mathrm{Fix}(\sigma)$, and $K_1(c)_{\sigma^{\pm 1}}$ is linearly disjoint from K_2 over K_1. In particular, if a is the generic of some $(V, \phi) \in AD_{K_2}$, then c is the generic of some $(W, \psi) \in AD_{K_1}$ with $\deg(\psi) = \deg(\phi)$. It is unlikely that such a c can always be found in $K_2(a)_{\sigma^{\pm 1}}$, but we do not know of a counterexample.

3. All results mentioned above generalize to the case where K_1 is not necessarily a subfield of K_2: for instance, in 3.3, the object (V_3, ϕ_3) will be defined over $K_0 = K_1^{alg} \cap K_2^{alg}$. If $K_0 \subset K_2$, then the (iso)morphism $(V_2, \phi_2) \to (V_3, \phi_3)$ is also defined over K_2.

The first section of the paper sets up the notation and recalls some of the classical results from stability theory and the model theory of existentially closed difference fields. In section 2, we prove some more technical results on difference fields, and in particular investigate quantifier-free types in reducts $(\mathcal{U}, \sigma^n)$ of our existentially closed difference field $\mathcal{U}$. Our two main results in this section are Proposition 2.14 and Theorem 2.17, and are we believe of independent interest. Finally, section 3 gives the proofs of the two main results.

1 Preliminaries on difference fields

1.1. Notation. A *difference field* is a field with a distinguished endomorphism σ. We denote by $\mathcal{L}$ the language of rings $\{+,-,\cdot,0,1\}$ and by $\mathcal{L}_\sigma$ the language $\mathcal{L}\cup\{\sigma\}$, where σ is a unary function symbol. Difference fields are then $\mathcal{L}_\sigma$-structures. Recall that a difference field is *inversive* if the endomorphism σ is also surjective.

Let $K\subset L$ be difference fields, E a field. If a is a tuple in L, then $K(a)_\sigma$ will denote the difference subfield of L generated by a over K: $K(a)_\sigma=K(\sigma^i(a)\mid i\in\mathbb{N})$; if K is inversive, then $K(a)_{\sigma^{\pm1}}$ will denote the inversive difference subfield of L generated by a: $K(a)_{\sigma^{\pm1}}=K(\sigma^i(a)\mid i\in\mathbb{Z})$. We denote by E^{sep} the separable closure of the field E, by E^{alg} its algebraic closure, and by $E^{\rm perf}$ the perfect hull E^{1/p^∞} over E if $\mathrm{char}(E)=p>0$, the field E if $\mathrm{char}(E)=0$. If F is a (finite) algebraic extension of E, then $[F:E]_s$ will denote the separable degree of F over E, and $[F:E]_i$ its inseparable degree. If the characteristic is $p>0$, then Frob will denote the Frobenius map $x\mapsto x^p$.

1.2. Existentially closed difference fields, the theory ACFA. The natural setting for studying difference equations is within existentially closed difference fields. A difference field $(\mathcal{U},\sigma)$ is *existentially closed* if any finite set of difference equations (over $\mathcal{U}$) with a solution in some difference field extension, already has a solution in $\mathcal{U}$.

The class of existentially closed difference fields is axiomatisable, and its theory is denoted by ACFA. All completions of ACFA are supersimple. We quickly recall some of the main properties of ACFA. For details, see [2]. Let $\mathcal{U}$ be an existentially closed difference field, K an inversive difference subfield of $\mathcal{U}$, and a a finite tuple of elements of $\mathcal{U}$.

(1) The *completions* of ACFA are obtained by specifying the characteristic and describing the isomorphism type of the algebraic closure of the prime field.

(2) If $A\subset\mathcal{U}$, then $\mathrm{acl}(A)$, the model-theoretic algebraic closure of A, coincides with the smallest algebraically closed inversive difference field containing A. Thus, for instance, if a is a tuple in $\mathcal{U}$, then $\mathrm{acl}(Ka)=K(a)^{alg}_{\sigma^{\pm1}}$.

(3) The model-theoretic definable closure of A (denoted by $\mathrm{dcl}(A)$) contains the inversive difference field generated by A, but is usually much larger, even when the characteristic is 0.

(4) Independence is defined using independence in the theory ACF of algebraically closed fields: A and B are *independent* over C ($A\perp_C B$) if and only if $\mathrm{acl}(CA)$ and $\mathrm{acl}(CB)$ are linearly disjoint over $\mathrm{acl}(C)$.

(5) The *quantifier-free type of a over K* describes the isomorphism type over K of $K(a)_{\sigma^{\pm1}}$, i.e.: $qftp(a/K)=qftp(b/K)$ if and only if there is a K-isomorphism of difference fields $K(a)_{\sigma^{\pm1}}\to K(b)_{\sigma^{\pm1}}$ which sends a to b (if and only if there is a K-isomorphism of difference fields $K(a)_\sigma\to K(b)_\sigma$ which sends a to b).

(6) The *type of a over K* describes the isomorphism type over K of the algebraic closure of Ka: $tp(a/K) = tp(b/K)$ if and only if there is a K-isomorphism of difference fields $\mathrm{acl}(Ka) \to \mathrm{acl}(Kb)$ which sends a to b.

(7) If a is an element of $\mathcal{U}$, then either the elements $\sigma^i(a)$, $i \in \mathbb{Z}$, are algebraically independent over K, in which case a is *transformally transcendental over K* and $SU(a/K) = \omega$; or the transcendence degree of $K(a)_{\sigma^{\pm 1}}$ over K is finite, i.e., a is *transformally algebraic over K*, and then $SU(a/K) < \omega$. Observe that if a is a tuple of elements which are transformally algebraic over K, then $SU(a/K) < \omega$, and for some m, $K(a)_{\sigma^{\pm 1}} \subset K(a, \sigma(a), \ldots, \sigma^m(a))^{alg} = \mathrm{acl}(Ka)$. In that case, we will often replace a by $(a, \sigma(a), \ldots, \sigma^m(a))$ and assume that $\sigma(a) \in K(a)^{alg}$.

(8) If $K = K^{alg}$ and L is a difference field containing K, there is a K-embedding of L into some elementary extension of $\mathcal{U}$.

For more properties of difference equations and of the theory ACFA, we refer to [2] and [3].

1.3. Conventions. Unless otherwise mentioned, all our difference fields will be **inversive**. This is in contrast with the first part, where the point of view was more geometric and thus it was convenient that difference fields arising from algebraic dynamics are finitely generated as fields; in this second part of the paper, the objects we are considering are difference fields and their algebraic closures, and it is more convenient for our purposes to have the smaller field be inversive. Observe for instance that if α is algebraic over K and $\sigma(K) = K$, then $[K(\alpha) : K] = [K(\sigma(\alpha)) : K]$; this is not necessarily the case if $\sigma(K) \neq K$. This is really just a matter of convenience and does not affect the generality of our results: every difference field has a unique (up to isomorphism) inversive closure, see Cohn's book [6], 2.5.II.

Unless otherwise mentioned, the letters a, b, x, y, ... will denote finite tuples of elements or variables, and we will abusively write e.g. $a \in K$ instead of a is a tuple of elements of K.

In the next few lemmas, we fix a difference subfield K of a *sufficiently saturated* existentially closed difference field $\mathcal{U}$. By sufficiently saturated, we mean that it is κ-saturated for some cardinal κ greater than all cardinalities of fields we consider, so that for instance, in item (8) above the K-embedding of L can be taken into $\mathcal{U}$.

1.4. Fixed fields. A *fixed field* is a subfield of $\mathcal{U}$ which is defined by the equation $\sigma^n(x) = x$, or by an equation of the form $\tau(x) = x$ where $\tau = \sigma^n \mathrm{Frob}^m$, $n > 0$, $m \in \mathbb{Z}$, if $char(\mathcal{U}) = p > 0$. The fixed field defined by $\tau(x) = x$ is denoted by $\mathrm{Fix}(\tau)$; it has SU-rank 1 if $n = 1$, or if $m \neq 0$ and n, m are relatively prime (see 7.1 in [3]). These conditions are clearly necessary, since $\mathrm{Fix}(\tau^\ell)$ is an ℓ-dimensional $\mathrm{Fix}(\tau)$-vector space.

Fact (see the proof of 3.7(3) in [2]). Let $\tau = \sigma^n \mathrm{Frob}^m$, and let a be a tuple in $\mathrm{Fix}(\tau)$. Then K and $\mathrm{Fix}(\tau)$ are linearly disjoint over their intersection, and therefore the field of definition of the algebraic locus of a over K is contained in $\mathrm{Fix}(\tau) \cap K^{\mathrm{perf}}$. In particular, if $a \in K^{alg}$ and b is the tuple encoding the set of field conjugates of a over K, then $b \in \mathrm{Fix}(\tau)$.

1.5. One-basedness. Recall that $\mathcal{U}$ eliminates imaginaries, see [2]. A subset S of $\mathcal{U}^n$ which is invariant under $\mathrm{Aut}(\mathcal{U}/K)$ is *one-based (over K)* if for any $K \subset L$ and tuple a of elements of S, a and L are independent over $\mathrm{acl}(Ka) \cap \mathrm{acl}(L)$. A partial type over K is one-based if the set of its realisations is one-based (thus any extension of a one-based type is one-based). In the presence of a finite dimension theory this is equivalent to the dimension inequality of Theorem 1.4 in [4]. The terms *modular* (used in [2], [3]) and *one-based* are thus synonymous; we will use the former when referring to (V, ϕ) itself, the latter for the solution set of $\sigma(x) = \phi(x)$. A finite union of one-based sets is one-based, and the same is true for uniformly definable unions: if $tp(a/K)$ and $tp(b/\mathrm{acl}(Ka))$ are one-based, then so is $tp(a, b/K)$ (see [2], [7] or in greater generality [8]). Types of infinite SU-rank are not one-based, nor are (non-algebraic) types which are realised in a fixed field. One important property is the following (see e.g. Lemma 3.3 in [2]):

Fact. Assume that $tp(a/K)$ is one-based, and L and K are independent over $K_0 \subset K, L$. Then $\mathrm{acl}(K_0a)$ and $\mathrm{acl}(L)$ are independent over their intersection.

1.6. The dichotomy. The main result of [3] asserts that if a is a tuple in $\mathcal{U}$ with $SU(a/K) = 1$, then $tp(a/K)$ is not one-based if and only if $tp(a/K)$ is non-orthogonal to a fixed field, i.e., there is some algebraically closed difference field L containing K and linearly disjoint from $K^{alg}(a)_{\sigma^{\pm 1}}$ over K^{alg}, such that $L(a)_{\sigma^{\pm 1}}$ contains a tuple $b \notin L$, b in some fixed field (non-orthogonality gives $b \in \mathrm{acl}(La)$, use Fact 1.4 to get $b \in L(a)_{\sigma^{\pm 1}}$).

1.7. Two definitions of internality. Let a be a tuple in $\mathcal{U}$, $a \notin K^{alg}$, and π a set of partial types (over various parameter sets) which is stable under $\mathrm{Aut}(\mathcal{U}/K)$.

(1) We say that $tp(a/K)$ is *qf-internal to* π if there is some $L = \mathrm{acl}(L)$ containing K and independent from a over K, and a tuple b of realisations of types in π with base contained in L and such that $a \in L(b)_{\sigma^{\pm 1}}$. (This notion is stronger than the usual notion of internality, which only requires $a \in \mathrm{dcl}(Lb)$).

(2) We say that $tp(a/K)$ is *almost internal to* π if there is some $L = \mathrm{acl}(L)$ containing K and independent from a over K, and a tuple b of realisations of types in π with base contained in L such that $a \in \mathrm{acl}(Lb)$.

By abuse of language, we also speak of qf-internality (or almost internality) to Π, where Π is the set of realisations of types in π. In practice, the set π will be a union of some of the following sets: non-algebraic 1-types containing $\tau(x) = x$ for some $\tau = \sigma^n \mathrm{Frob}^m$; all one-based types of SU-rank 1.

1.8. Internality to a fixed field. Assume that Π is the fixed field $\mathrm{Fix}(\tau)$. Using Fact 1.4, one easily deduces

(1) $tp(a/K)$ is qf-internal to $\mathrm{Fix}(\tau)$ if and only if for some L independent from a over K, $L(a)_{\sigma^{\pm 1}} = L(b)_{\sigma^{\pm 1}}$ for some $b \in \mathrm{Fix}(\tau)$.

(2) $tp(a/K)$ is almost internal to $\mathrm{Fix}(\tau)$ if and only if for some L independent from a over K and for some tuple b in $\mathrm{Fix}(\tau) \cap L(a)_{\sigma^{\pm 1}}$, $a \in \mathrm{acl}(Lb)$.

Remarks.

(1) Observe that being qf-internal to $\tau(x) = x$ or to $\tau^k(x) = x$ is the same thing, because $\mathrm{Fix}(\tau^k)$ is a k-dimensional vector space over $\mathrm{Fix}(\tau)$ and therefore $\mathrm{Fix}(\tau^k) = \mathrm{Fix}(\tau)(b)$ if b is any $\mathrm{Fix}(\tau)$-basis of $\mathrm{Fix}(\tau^k)$.

(2) For algebraic dynamics, this notion is called *field-internal* in [4], and *fixed-field-internal* if $\tau = \sigma$.

1.9. Analyses. Let $K = \mathrm{acl}(K) \subset \mathcal{U}$, a a tuple in $\mathcal{U}$, with $SU(a/K)$ finite. A tuple (of tuples) $(a_1, \ldots, a_n)$ is a *semi-minimal analysis* of a over K (or of $tp(a/K)$) iff $\mathrm{acl}(Ka_1, \ldots, a_n) = \mathrm{acl}(Ka)$, and for every i, $tp(a_i/\,\mathrm{acl}(Ka_1, \ldots, a_{i-1}))$ is (almost- or qf-) internal to the set of conjugates of a type of SU-rank 1.

By general properties of supersimple theories, every finite SU-rank type has a semi-minimal analysis. If it is one-based, then one can find an analysis in which all types $tp(a_i/\,\mathrm{acl}(Ka_1, \ldots, a_{i-1}))$ have SU-rank 1.

The properties of one-based types and the dichotomy (see 1.5 and 1.6) then yield:

Fact. A type of finite SU-rank is one-based if and only if it has a semi-minimal analysis in which all types are one-based types, if and only if any of its extensions is orthogonal to all fixed fields, if and only if any of its semi-minimal analyses only involves types orthogonal to all fixed fields.

Recall that a type is *hereditarily orthogonal* to a set π of types, if all its extension are orthogonal to all members of π. Thus another way of rephrasing the previous fact is: a type is one-based if and only if it is hereditarily orthogonal to all (types realised in) fixed fields. In the context of algebraic dynamics, this corresponds to *field-free*, see [4].

1.10. The limit degree and the inverse limit degree. These are numerical invariants that will be helpful in proving closure properties of AD_K within the category of difference varieties over K. Indeed, an object $(V, \phi) \in AD_K$ will correspond to difference field extensions with limit degree 1 and inverse limit degree $\deg(\phi)$.

Definition. Let a be a tuple in $\mathcal{U}$, and assume that $\sigma(a) \in K(a)^{alg}$. The *limit degree of a over K* (or of $K(a)_{\sigma^{\pm 1}}$ over K) is

$$ld(a/K) = \lim_{k\to\infty} [K(a, \sigma(a), \ldots, \sigma^{k+1}(a)) : K(a, \sigma(a), \ldots, \sigma^k(a))],$$

and the *inverse limit degree of a over K* is

$$ild(a/K) = \lim_{k\to\infty} [K(a, \sigma^{-1}(a), \ldots, \sigma^{-(k+1)}(a)) : K(a, \sigma^{-1}(a), \ldots, \sigma^{-k}(a))].$$

The limit and inverse limit degrees are invariants of the extension $K(a)_{\sigma^{\pm 1}}/K$, see [6], section 5.16. If $[K(a, \sigma(a)) : K(a)] = ld(a/K)$, then the fields $K(\sigma^i(a) \mid i \leq 0)$ and $K(\sigma^i(a) \mid i \geq 0)$ are linearly disjoint over $K(a)$, and $ild(a/K) = [K(a, \sigma(a)) : K(\sigma(a))]$. Another important property is that these degrees are multiplicative in tower.

Lemma 1.11. *Let a and b tuples in $\mathcal{U}$ such that $b, \sigma(a) \in K(a)^{alg}$ and $\sigma(b) \in K(b)^{alg}$.*

(1) *If $b \in K(a)_{\sigma^{\pm 1}}$, then $ld(b/K) \leq ld(a/K)$ and $ild(b/K) \leq ild(a/K)$.*

(2) *If $a \in K^{alg}$, then $ld(a/K) = ild(a/K)$.*

(3) *If $ld(b/K) = 1$, then $K(a,b)_{\sigma^{\pm 1}}$ is a finite extension of $K(a)_{\sigma^{\pm 1}}$.*

(4) *If some analysis of $tp(a/K)$ only involves types non-orthogonal to* $\mathrm{Fix}(\sigma)$*, then $ld(a/K) = ild(a/K)$.*

Proof. (1) Follows from $ld(a,b/K) = ld(a/K) = ld(a/K(b)_{\sigma^{\pm 1}})ld(b/K)$, and similarly for ild.

(2) Replacing a by $(a, \dots, \sigma^m(a))$ for some m, we may assume that $ld(a/K) = [K(a, \sigma(a)) : K(a)]$ so that also $[K(a, \sigma(a)) : K(\sigma(a))] = ild(a/K)$. Then $[K(a) : K] = [K(\sigma(a)) : K]$ gives the result.

(3) By (2), $ild(b/K(a)_{\sigma^{\pm 1}}) = ld(b/K(a)_{\sigma^{\pm 1}}) = 1$; hence, for some m, $K(a,b)_{\sigma^{\pm 1}} = K(a)_{\sigma}(b, \sigma(b), \dots, \sigma^m(b))$.

(4) We know that the limit and inverse limit degrees are multiplicative in tower. By (2), $ld(b/K)/ild(b/K) = ld(b/K^{alg})/ild(b/K^{alg})$ is an invariant of the extension $K(b)_{\sigma}^{alg}/K$. Thus the result holds if $tp(a/K)$ is almost internal to $\mathrm{Fix}(\sigma)$: by assumption there are $L = \mathrm{acl}(L)$ independent from a over K and a tuple $b \in \mathrm{Fix}(\sigma)$ such that $\mathrm{acl}(La) = \mathrm{acl}(Lb)$. Since $ld(b/L) = ild(b/L) = 1$, we have $ld(a/L) = ild(a/L)$; because a and L are independent over K, we have $ld(a/K^{alg}) = ld(a/L)$ and $ild(a/K^{alg}) = ild(a/L)$. By induction on the length of a semi-minimal analysis of $tp(a/K)$, we get the result. ☐

2 From types to isomorphism types

As defined in [2], [3], modularity and fixed-field internality were properties of a complete type $tp(c/K)$ in a saturated model $\mathcal{U}$ of ACFA. We show here that they actually depend only on the difference field extension $K(c)_{\sigma^{\pm 1}}/K$. In the section 2 of the first part [4], we present the same material differently, defining the notions directly in a way that does not use the embedding.

We fix two sufficiently saturated models $\mathcal{U}$ and $\mathcal{U}'$ of ACFA, and a difference subfield K of $\mathcal{U}$. Unless otherwise specified, τ will always be an automorphism of the form $\sigma^m\mathrm{Frob}^n$, with $m = 0$ and $n = 1$, or $(m,n) = 1$, so that $SU(\mathrm{Fix}(\tau)) = 1$. We will usually be working in $\mathcal{U}$, when working in $\mathcal{U}'$ we will indicate it by a subscript $\mathcal{U}'$.

2.1. Reducts. If k is a positive integer, we denote by $\mathcal{U}[k]$ the reduct $(\mathcal{U}, \sigma^k)$ of the difference field $\mathcal{U}$. It is also an existentially closed difference field (Corollary 1.12(1) in [2]). If a is a tuple in $\mathcal{U}$, then we denote by $qftp(a/K)[k]$, $tp(a/K)[k]$, $SU(a/K)[k]$ respectively the quantifier-free type, type and SU-rank of the tuple a over K in $\mathcal{U}[k]$. We will denote by $\mathrm{acl}_{\sigma^k}(A)$ the algebraic closure in the sense of $\mathcal{U}[k]$.

2.2. Codes. Recall that if $a_1, \dots, a_m$ are n-tuples in some field, then the code of the set $\{a_1, \dots, a_m\}$ is defined as the tuple b of coefficients of the polynomial $\prod_{i=1}^m (X_0 + a_i \cdot X)$, where $X = (X_1, \dots, X_n)$ and $\cdot$ is the usual dot product of vectors in n-space.

If the tuple a is separably algebraic over the field E, and $a = a_1, a_2, \dots, a_m$ are the distinct field conjugates of a over E, then the code b of $\{a_1, \dots, a_m\}$ belongs to E. If a is only algebraic over E, then some p-th power of b will belong to E.

2.3. The field of definition of the difference locus. Let L be a difference overfield of K, and a an n-tuple in $\mathcal{U}$. We define the *difference locus of a over L* to be the smallest subset of $\mathcal{U}^n$ defined by difference equations over L and containing a.

We define the *field of definition of the difference locus of a over L* to be the smallest difference subfield E of $L^{\rm perf}$ such that $E(a)_{\sigma^{\pm 1}}$ and $L^{\rm perf}$ are linearly disjoint over E, and denote it by qf-Cb(a/L). It can also be described as the field of definition of the algebraic locus of the infinite tuple $\{\sigma^i(a) \mid i \in \mathbb{Z}\}$ over $L^{\rm perf}$.

We define the *field of definition of the difference locus of the tuple a over L/K* to be the smallest difference subfield E of $L^{\rm perf}$ which contains K and is such that $E(a)_{\sigma^{\pm 1}}$ and $L^{\rm perf}$ are linearly disjoint over E and denote it by qf-Cb$_K(a/L)$; note that qf-Cb$_K(a/L) = K$qf-Cb(a/L).

2.4. Warning. Let a, $K \subset L$ as above. An important observation is that qf-Cb(a/L) is not necessarily contained in L, but may be purely inseparable over L. In positive characteristic, it is therefore *not to be confused* with the field of definition of the σ-ideal of difference polynomials over L vanishing at a, which is contained in L, and can be defined as the smallest subfield E' of L such that $E'(a)_{\sigma^{\pm 1}}$ and L are linearly disjoint over E'. In positive characteristic, the two fields of definition are different, it may even happen that E' is not algebraic over qf-Cb(a/L)!

Here is a purely algebraic example where this phenomenon occurs: let a, b, t be algebraically independent over $\mathbb{F}_p$. Let $K = \mathbb{F}_p(a^p, b^p, t, a + bt)$, and consider the point (a, b). Then qf-Cb$(a, b/K) = \mathbb{F}_p(a, b)$; however, K is the field of definition of the ideal $I(a, b/K) = (X^p - a^p, Y^p - b^p, X + tY - (a + bt))$.

2.5. More properties of qf-Cb. Let a, $K \subset L$ as above, and let k be the prime field.

(1) As in the algebraic case, the field qf-Cb(a/L) is contained in the difference field generated by realisations of $qftp_{\rm ACF}((\sigma^i(a)_{i\in\mathbb{Z}})/L)$, where $qftp_{\rm ACF}$ denotes the type in the reduct to the language of rings. Also, if $L(a)_{\sigma^{\pm 1}} \cap L^{sep} = L$ (i.e., if $L(a)_{\sigma^{\pm 1}}$ is a *primary* extension of L), then there is a unique quantifier-free type over L^{alg} extending $qftp(a/L)$: this is because $qftp_{\rm ACF}(\sigma^i(a)_{i\in\mathbb{Z}})/L)$ is stationary. In that case, qf-Cb(a/L) is contained in the difference field generated by finitely many realisations of $tp(a/L)$.

(2) Assume now that $L(a)_{\sigma^{\pm 1}}/L$ is not primary. Then for some ℓ, qf-Cb(a/L) is contained in the difference field generated by finitely many realisations of qf-Cb$(a/L)[\ell]$.

(3) If $L(a)/L$ is separable, then qf-Cb$(a/L) \subset L$.

(4) By 5.23.XVIII of [6], qf-Cb(a/L) is finitely generated as a (σ^ℓ-)difference field, since it is contained in a finitely generated one.

Proof. (1) and (2). We will use the following classical facts for algebraic sets: let V be an absolutely irreducible variety. Then for some m, if $a_1, \dots, a_m$ are independent generics of V, the field generated by $a_1, \dots, a_m$ contains the field of definition of V. Assume now that V is L-irreducible, but not necessarily absolutely irreducible; let V_0 be an absolutely irreducible component of V, and $k(b)$ its field of definition. Then the field generated by the field conjugates of b over L contains the field of definition of V, since it contains the fields of definitions of all irreducible components of V.

By 3.8.V of [6], the topology on cartesian powers of $\mathcal{U}$ with closed sets the zero-sets of difference polynomials over $\mathcal{U}$ is Noetherian; hence there is an integer m such that if $(b, \sigma(b), \dots, \sigma^m(b))$ has the same algebraic locus over L as $(a, \sigma(a), \dots, \sigma^m(a))$, then a and b have the same difference locus over L. This implies that if the tuple c generates the field of definition of the algebraic locus of $(a, \dots, \sigma^m(a))$ over L, then $k(c)_{\sigma^{\pm 1}} = \text{qf-Cb}(a/L)$. If $L(a)_{\sigma^{\pm 1}}/L$ is primary, then the difference locus of a over L is absolutely irreducible, hence, taking finitely many generic independent realisations of $tp(a/L)$, we obtain (1).

Let us now prove (2). Let m be as above, and c such that $k(c)$ is the field of definition of the algebraic locus of $(a, \sigma(a), \dots, \sigma^m(a))$ over L^{alg}. Then the field of definition of the algebraic locus of $(a, \sigma(a), \dots, \sigma^m(a))$ is contained in the field generated by the set of (field-) conjugates of c over L. Hence, by the definition of m, $\text{qf-Cb}(a/L)$ is contained in the difference field generated by these field conjugates of c over L. By (1.12) of [3], for some ℓ, if c' is a field conjugate of c over L, then $qftp(c'/L)[\ell] = qftp(c/L)[\ell]$. This gives the result.

(3) follows from the fact that $L(a)_{\sigma^{\pm 1}}$ and L^{perf} are linearly disjoint over L, and (4) is clear. □

The following algebraic lemma will be useful

2.6. Lemma. Let $K \subset L_0 \subset L$, $K \subset M$ and N be fields, such that L and M are linearly disjoint over K, L/L_0 is algebraic, M/K is regular, and $L_0M \subset N \subset LM$. Then $N = L_1M$ where $L_1 = L \cap N$ in each of the following cases:

(a) if N/L_0M is separable, or

(b) (char. $p > 0$) if $[L_0 : L_0^p] = p$ (for instance, if $tr.deg(L/K) = 1$ and K is perfect).

Proof. We may assume that L/L_0 is finite, since if the conclusion is false it will be witnessed by a finite subextension.

(a) This is well-known: without loss of generality, L is separable over L_0; let $\hat{L}$ be the Galois closure of L over L_0. Then the regularity of M/K and the independence of L and M over K imply that $\hat{L}$ and M are linearly disjoint over K; hence fields between L_0M and LM correspond to groups between $\mathcal{G}al(\hat{L}M/LM) \simeq \mathcal{G}al(\hat{L}/L)$ and $\mathcal{G}al(\hat{L}M/L_0M) \simeq \mathcal{G}al(\hat{L}/L_0)$. The result follows.

(b) Using a tower of extensions and the first case, we may assume that N/L_0M is purely inseparable of degree p, and L/L_0 is purely inseparable. Since $[L_0^p : L_0] = p$, we get $L \supset L_0^{1/p}$ and our linear disjointness assumption implies that L_0M/L_0 is separable (as L and L_0M are

linearly disjoint over L_0). This implies that $N \subseteq L_0^{1/p}M$: assume not, write $N = L_0M(c)$ where $c^p \in L_0M$, and let $a \in L_0 \setminus L_0^p$; if $c \notin L_0^{1/p}M$, then c, a are p-independent, and this implies that $c \notin L_0(a^{1/p^n})$ for any n; i.e., $c \notin L_0^{\mathrm{perf}}M$, which gives us the desired contradiction. $\square$

Lemma 2.7. *Let $k \geq 1$, and (L, σ^k) be a finitely generated σ^k-difference field extending (K, σ^k), and such that L is a primary extension of K. Then there is a K-embedding of the σ^k-difference field L into $\mathcal{U}[k]$.*

Proof. Since $\mathcal{U}[k]$ is also a saturated model of ACFA, it suffices to show the result for $k = 1$.

The automorphism σ extends uniquely to K^{perf}, and we may therefore assume that K is perfect. Our primarity hypothesis now implies that L and K^{alg} are linearly disjoint over K, and therefore that $L \otimes_K K^{alg}$ is a field. Defining σ on $L \otimes_K K^{alg}$ so that it extends $\sigma|_{K^{alg}}$ and $\sigma|_L$, we use 1.2(8) to conclude. $\square$

Lemma 2.8. *Let a be a tuple in $\mathcal{U}$, and assume that $tp(a/K)$ is qf-internal to $\mathrm{Fix}(\tau)$. Then there is a tuple c of realisations of $tp(a/K^{alg})$ such that if $L = K(c)_{\sigma^{\pm 1}}$, then $L(a)_{\sigma^{\pm 1}}$ is a primary extension of $K(a)_{\sigma^{\pm 1}}$, $L \downarrow_K a$, and $L(a)_{\sigma^{\pm 1}} = L(b)_{\sigma^{\pm 1}}$ for some tuple b in $\mathrm{Fix}(\tau)$.*

Proof. By assumption there is some $L' = \mathrm{acl}(L')$ independent from a over K, and such that $L'(a)_{\sigma^{\pm 1}} = L'(b)_{\sigma^{\pm 1}}$ for some tuple b in $\mathrm{Fix}(\tau)$.

Let $(a_i, b_i)_{i \in \mathbb{N}}$ be an independent sequence of realisations of $tp(a, b/L')$, with $(a_0, b_0) = (a, b)$. Then for some n, $K(a_1, b_1, \ldots, a_n, b_n)_{\sigma^{\pm 1}}$ contains qf-$\mathrm{Cb}_K(a, b/L')$. Let $L = K(a_1, \ldots, a_n)_{\sigma^{\pm 1}}$. Then $L(a, b_1, \ldots, b_n)_{\sigma^{\pm 1}} = L(b, b_1, \ldots, b_n)_{\sigma^{\pm 1}}$, i.e., $L(a)_{\sigma^{\pm 1}} \subset L\mathrm{Fix}(\tau)$. Observe that L and $K(a)^{sep}_{\sigma^{\pm 1}}$ are linearly disjoint over $K(a)_{\sigma^{\pm 1}} \cap K^{sep}$: this is because the a_i's are independent realisations of $tp(a/L')$, and in particular of $tp(a/K^{alg})$, and because $a \downarrow_K L'$. Hence $L(a)_{\sigma^{\pm 1}}$ is a primary extension of $K(a)_{\sigma^{\pm 1}}$, and is generated over K by realisations of $tp(a/K^{alg})$. $\square$

Proposition 2.9. *Let $a \in \mathcal{U}$ and ℓ a positive integer, $\mathrm{Fix}(\tau)$ a fixed field.*

1. *Assume that $tp(a/K)$ is qf-internal to $\mathrm{Fix}(\tau)$. Also, assume that $\varphi : K(a)_{\sigma^{\pm 1}} \to K'(a')_{\sigma^{\pm 1}} \subset \mathcal{U}'$ is an isomorphism with $\varphi(K) = K'$, $\varphi(a) = a'$. Then $tp_{\mathcal{U}'}(a'/K')$ is qf-internal to $\mathrm{Fix}(\tau)$.*

2. *$tp(a/K)[\ell]$ is qf-internal to $\mathrm{Fix}(\tau^\ell)$ if and only if $tp(a/K)$ is qf-internal to $\mathrm{Fix}(\tau)$.*

Proof. (1) Apply Lemmas 2.8 and 2.7 (with $k = 1$).

(2) Assume first that $tp(a/K)$ is qf-internal to $\mathrm{Fix}(\tau)$. Then $tp(a/K)[\ell]$ is qf-internal to $\mathrm{Fix}(\tau^\ell)$ because $\mathrm{Fix}(\tau) \subset \mathrm{Fix}(\tau^\ell)$: by hypothesis there is $L = \mathrm{acl}(L)$ which is independent from a over K and such that $a \in L\mathrm{Fix}(\tau) \subset L\mathrm{Fix}(\tau^\ell)$.

Assume now that $tp(a/K)[\ell]$ is qf-internal to $\mathrm{Fix}(\tau^\ell)$. Then so are $tp(\sigma^i(a)/K)[\ell]$ for all i, and, replacing a by $(a, \sigma(a), \ldots, \sigma^m(a))$ for some m, we may therefore assume that $\sigma(a) \in K(a)^{alg}$, and $K(a)_{\sigma^{\pm 1}} = K(a)_{\sigma^{\pm \ell}}$. By 2.8, in $\mathcal{U}[\ell]$, there is a σ^ℓ-difference field L such that $L(a)_{\sigma^{\pm \ell}} \subset L\mathrm{Fix}(\tau^\ell)$, $L \downarrow_K a$, and $L(a)_{\sigma^{\pm \ell}}/K(a)_{\sigma^{\pm \ell}}$ is primary. However, it may be that the σ-difference subfield of $\mathcal{U}$ generated by L is not independent from a over K. Since σ and σ^ℓ extend

uniquely to the perfect closure of a field, we may assume that L and K are perfect, so that now $L(a)_{\sigma^{\pm\ell}}$ is a regular extension of $K(a)_{\sigma^{\pm\ell}} = K(a)_{\sigma^{\pm1}}$. For each $i = 0, \dots, \ell - 1$, we choose L_i realising $\sigma^i(tp(L/K(a)_{\sigma^{\pm1}})[\ell])$ and such that $L_0 = L$, $L_1, \dots, L_{\ell-1}$ are independent over $K(a)_{\sigma^{\pm\ell}} = K(a)_{\sigma^{\pm1}}$. Since they are isomorphic copies of the regular extension $L(a)_{\sigma^{\pm\ell}}/K(a)_{\sigma^{\pm1}}$, they are in fact linearly disjoint over $K(a)_{\sigma^{\pm1}}$. Hence, reasoning as in 1.12 of [2], we can define an extension ρ of σ on the composite field $L_0 \cdots L_{\ell-1}$, such that ρ^ℓ coincides with σ^ℓ on L_0. Thus, by Lemma 2.7, there is a $K(a)_{\sigma^{\pm1}}$-embedding φ of the σ-difference field $(L_0 \cdots L_{\ell-1}, \rho)$ into $\mathcal{U}$; then $a \in \varphi(L)\mathrm{Fix}(\tau^\ell)$, and we are done. □

Lemma 2.10. *Let a be a tuple in $\mathcal{U}$, and assume that $tp(a/K)$ is non-orthogonal to* $\mathrm{Fix}(\tau)$*. Then there is $e \in K(a)_{\sigma^{\pm1}}$ such that $tp(e/K)$ is qf-internal to* $\mathrm{Fix}(\tau)$*.*

Proof. By assumption (and Fact 1.4) there are tuples b and c, with $c \mathop{\smile\!\!\!\!\!\!\,|}_K a$, $b \in \mathrm{Fix}(\tau)$, and $b \in K(c,a)_{\sigma^{\pm1}}$, $b \notin K(c)^{alg}_{\sigma^{\pm1}}$. Reason exactly as in the proof of 2.8 to show that c can be chosen so that $K(c,a)_{\sigma^{\pm1}}$ is a primary extension of $K(a)_{\sigma^{\pm1}}$. As $b \in K(a,c)_{\sigma^{\pm1}}$, it follows that qf-$\mathrm{Cb}_K(b,c/K(a)_{\sigma^{\pm1}})$ is contained in the difference field generated by independent realisations of $tp(b,c/K(a)_{\sigma^{\pm1}})$, i.e., if $K(e)_{\sigma^{\pm1}} =$ qf-$\mathrm{Cb}_K(b,c/K(a)_{\sigma^{\pm1}})$, then $tp(e/K)$ is qf-internal to $\mathrm{Fix}(\tau)$. For some n, $e^{p^n} \in K(a)_{\sigma^{\pm1}}$. □

Proposition 2.11. *Let a be a tuple in $\mathcal{U}$, and ℓ a positive integer.*

(1) *$tp(a/K)$ is one-based if and only if $tp(a/K)[\ell]$ is one-based.*

(2) *If $\varphi : K(a)_{\sigma^{\pm1}} \to K'(a')_{\sigma^{\pm1}} \subset \mathcal{U}'$ is an isomorphism with $\varphi(K) = K'$, $\varphi(a) = a'$, and if $tp(a/K)$ is one-based, then so is $tp_{\mathcal{U}'}(a'/K')$.*

(3) *If $tp(a/K)$ is non-orthogonal to a one-based type, then there is $b \in K(a)_{\sigma^{\pm1}}$ such that $tp(b/K)$ is one-based.*

Proof. (1) Assume first that $tp(a/K)[\ell]$ is one-based, let $\bar{a}$ be a tuple of realisations of $tp(a/K)$, and $L = \mathrm{acl}(L) \supset K$. Observe that for each i, $tp(\sigma^i(a)/K)[\ell]$ is also one-based, and therefore so is $tp(\bar{a}, \sigma(\bar{a}), \dots, \sigma^{\ell-1}(\bar{a})/K)[\ell]$. Hence $\mathrm{acl}_{\sigma^{\pm\ell}}(K, \bar{a}, \sigma(\bar{a}), \dots, \sigma^{\ell-1}(\bar{a})) = \mathrm{acl}(K\bar{a})$ and L are linearly disjoint over their intersection. This shows that $tp(a/K)$ is one-based.

Assume that $tp(a/K)$ is one-based, but not $tp(a/K)[\ell]$. Replacing a by $(a, \sigma(a), \dots, \sigma^m(a))$ for some m, we may assume that $\sigma(a) \in K(a)^{alg}$ and $K(a)_{\sigma^{\pm1}} = K(a)_{\sigma^{\pm\ell}}$. Then, using the semi-minimal analysis in $\mathcal{U}[\ell]$ and the trichotomy, there is $c \in K(a)^{alg}$ such that $tp(c/K)[\ell]$ is one-based, and $tp(a/K(c)_{\sigma^{\pm\ell}})[\ell]$ is non-orthogonal to $\mathrm{Fix}(\tau^\ell)$ for some fixed field $\mathrm{Fix}(\tau)$. Then also each $tp(\sigma^i(c)/K)[\ell]$ is one-based, and therefore $tp(a/K(c)_{\sigma^{\pm1}})[\ell]$ is non-orthogonal to $\mathrm{Fix}(\tau^\ell)$ as well (see 1.5). Enlarging c, we may assume that $K(c)_{\sigma^{\pm1}} = K(c)_{\sigma^{\pm\ell}}$. By Lemma 2.10, there is a tuple $b \in K(c,a)_{\sigma^{\pm\ell}}$ such that $tp(b/K(c)_{\sigma^{\pm\ell}})[\ell]$ is qf-internal to $\mathrm{Fix}(\tau^\ell)$. Since $K(c)_{\sigma^{\pm1}} = K(c)_{\sigma^{\pm\ell}}$, Lemma 2.8 gives $tp(b/K(c)_{\sigma^{\pm1}})$ qf-internal to $\mathrm{Fix}(\tau)$, which contradicts the one-basedness of $tp(a/K)$.

(2) We may assume that $\sigma(a) \in K(a)^{alg}$. The proof is by induction on $tr.deg(K(a)_{\sigma^{\pm1}}/K)$. If it is 0, there is nothing to prove. Assume that $tp_{\mathcal{U}'}(a'/K')$ is not one-based. Then there

is $c' \in K'(a')^{alg}$ such that $tp_{\mathcal{U}'}(c'/K')$ is one-based, and $tp_{\mathcal{U}'}(a'/K(c')_{\sigma^{\pm 1}})$ is non-orthogonal to some fixed field $\mathrm{Fix}(\tau)$. We may assume that $\sigma(c') \in K'(c')^{alg}$, and that either $c' \notin K'^{alg}$, or $c' \in K'$.

If $c' \in K'$, then Lemma 2.10 and Proposition 2.9 imply $tp(a/K)$ non-orthogonal to $\mathrm{Fix}(\tau)$, a contradiction.

Assume that $c' \notin K'$. By 1.12(3) of [3], there are $\ell \geq 1$ and $c \in \mathcal{U}$ such that φ extends to a σ^ℓ-isomorphism $\varphi : K(a)_{\sigma^{\pm 1}}(c)_{\sigma^{\pm \ell}} \to K(a')_{\sigma^{\pm 1}}(c')_{\sigma^{\pm \ell}}$. Since $\sigma(c') \in K'(c')^{alg}$, $tp_{\mathcal{U}'}(a'/K(c')_{\sigma^{\pm \ell}})[\ell]$ is non-orthogonal to $\mathrm{Fix}(\tau^\ell)$. By Lemma 2.10 and Proposition 2.9, so is $tp(a/K(c)_{\sigma^{\pm \ell}})[\ell]$. As $tr.deg(K'(c')_{\sigma^{\pm 1}}/K') < tr.deg(K'(a')_{\sigma^{\pm 1}}/K')$, by induction hypothesis, we know that $tp(c/K)[\ell]$ is one-based, as are all $tp(\sigma^i(c)/K)[\ell]$. Hence, $tp(a/K(c)_{\sigma^{\pm 1}})[\ell]$ is non-orthogonal to $\mathrm{Fix}(\tau^\ell)$. We then reason as in the previous case to get a contradiction.

(3) Our assumption implies that there is $c \in \mathrm{acl}(Ka)$ with $tp(c/K)$ one-based (see 1.9). Let $c = c_1, c_2, \ldots, c_m$ be the distinct field conjugates of c over $K(a)_{\sigma^{\pm 1}}$. By 1.12 of [3], there is $\ell \geq 1$ such that they all have the same quantifier-free type over K in $\mathcal{U}[\ell]$. By (1), $tp(c/K)[\ell]$ is one-based, and by (2), so are $tp(c_i/K)[\ell]$ for $i \geq 1$. Hence if $b \in K(a)_{\sigma^{\pm 1}}$ is (some p^n-power of) the code of the set $\{c_1, \ldots, c_m\}$, then $tp(b/K)[\ell]$ is one-based, and so is $tp(b/K)$. □

2.12. Definition. Let a be a tuple in $\mathcal{U}$. We say that $K(a)_{\sigma^{\pm 1}}/K$ is *primitive* if $tr.deg(K(a)_{\sigma^{\pm 1}}/K) < \infty$, and whenever $b \in K(a)_{\sigma^{\pm 1}}$, then either $b \in K^{alg}$ or $a \in K(b)_{\sigma^{\pm 1}}^{alg}$. (This agrees with the definition of primitive algebraic dynamics given in [4].)

The previous results 2.10, 2.9 and 2.11 then immediately yield:

Proposition 2.13. *Assume that $K(a)_{\sigma^{\pm 1}}/K$ is primitive and of finite transcendence degree (over K). Then*

(1) *either $tp(a/K)$ is one-based,*

(2) *or there is $d \in K(a)_{\sigma^{\pm 1}}$ such that $tp(d/K)$ is qf-internal to some fixed field $\mathrm{Fix}(\tau)$ and $a \in K(d)_{\sigma^{\pm 1}}^{alg}$.*

(3) *Whether (1) or (2) holds only depends on the isomorphism type of the difference field extension $K(a)_{\sigma^{\pm 1}}/K$, i.e.: let $\varphi : K(a)_{\sigma^{\pm 1}} \to K'(a')_{\sigma^{\pm 1}} \subset \mathcal{U}'$ be an isomorphism with $\varphi(K) = K'$, $\varphi(a) = a'$. Then $tp(a/K)$ is one-based [resp. $tp(d/K)$ is qf-internal to $\mathrm{Fix}(\tau)$ and $a \in K(d)_{\sigma^{\pm 1}}^{alg}$] if and only if $tp_{\mathcal{U}'}(a'/K')$ is one-based [resp. if $d' = \varphi(d)$, then $tp_{\mathcal{U}'}(d'/K')$ is qf-internal to $\mathrm{Fix}(\tau)$ and $a' \in K'(d')_{\sigma^{\pm 1}}^{alg}$].*

Clearly, given some tuple a, one can find tuples $a_1, \ldots, a_n \in K(a)_{\sigma^{\pm 1}}$ such that $K(a)_{\sigma^{\pm 1}} = K(a_1, \ldots, a_n)_{\sigma^{\pm 1}}$, and for each i, $K(a_1, \ldots, a_i)_{\sigma^{\pm 1}}/K(a_1, \ldots, a_{i-1})_{\sigma^{\pm 1}}$ is either primitive or algebraic. Thus, Proposition 2.13 has the following immediate consequence:

Theorem 2.14. *Assume that a has finite SU-rank over K. Then there are $a_1, \ldots, a_n$ such that $K(a_1, \ldots, a_n)_{\sigma^{\pm 1}} = K(a)_{\sigma^{\pm 1}}$, and for each i, $tp(a_i/K(a_1, \ldots, a_{i-1})_{\sigma^{\pm 1}})$ is of one of the following three kinds:*

(a) *algebraic,*

(b) *one-based,*

(c) *qf-internal to* $\mathrm{Fix}(\tau)$ *for some* τ.

2.15. These results have many easy consequences. Let us mention two, others can be derived in a similar way. We fix a subset π of

$$\{(\sigma^n(x^{p^m}) = x : (n,m) = 1, n > 0\} \cup \{\{\text{all one-based types of SU-rank 1}\}\}.$$

Proposition 2.16. *Let a be a tuple, $\ell \geq 1$, E a difference subfield of $\mathcal{U}$, and assume that $tp(a/K)$ is π-analysable.*

(1) *Then so is $qftp(a/K)[\ell]$.*

(2) *If $a \in E^{alg}$, and b is a code for the set of field conjugates of a over E, then so is $tp(b/K)$.*

(3) *Let $\varphi : K(a)_{\sigma^{\pm 1}} \to K'(a')_{\sigma^{\pm 1}} \subset \mathcal{U}'$ be an isomorphism with $\varphi(K) = K'$, $\varphi(a) = a'$. Then $tp_{\mathcal{U}'}(a'/K')$ is π-analysable.*

(4) *Statements (1), (2) and (3) hold if one replaces π-analyzable by qf-internal to π.*

Proof. (1) Let $(a_1, \ldots, a_n) \in K(a)_{\sigma^{\pm 1}}$ satisfy the conclusion of Theorem 2.14 for the extension $K(a)_{\sigma^{\pm 1}}/K$. Then by Propositions 2.9 and 2.11 so does the tuple $(a_1, \sigma(a_1), \ldots, \sigma^{\ell-1}(a_1), a_2, \sigma(a_2), \ldots, \sigma^{\ell-1}(a_n))$ for the extension $K(a, \sigma(a), \ldots, \sigma^{\ell-1}(a))_{\sigma^{\pm\ell}}/K$ in $\mathcal{U}[\ell]$. As $K(a)_{\sigma^{\pm\ell}} \subset K(a)_{\sigma^{\pm 1}}$, this gives the result.

(2) By 1.12 of [3], for some ℓ, all field conjugates of a over E satisfy the same quantifier-free type in $\mathcal{U}[\ell]$. The result follows from (1).

(3) Clear from Theorem 2.14 and Proposition 2.13,

(4) Identical proof. $\square$

Theorem 2.17. *Let $K \subset L$ be difference fields, and a a tuple. Let π be a set of types as above. Let $b \in L^{\mathrm{perf}}$ be such that $K(b)_{\sigma^{\pm 1}} = qf\text{-}Cb_K(a/L)$. Assume that there is some $c \in K(a)_{\sigma^{\pm 1}}$ which is independent from L over K and such that $tp(a/K(c)_{\sigma^{\pm 1}})$ is π-analysable. Then so is $tp(b/K)$.*

Proof. Let d be such that $K(d)_{\sigma^{\pm 1}} = \mathrm{qf\text{-}Cb}_K(a/L^{alg})$. As $c \in K(a)_{\sigma^{\pm 1}}$, d is contained in the difference field generated over K by a tuple (c^1, a^1) of finitely many L-independent realisations of $tp(c, a/L^{alg})$. As $c \perp_K L$, it follows that $tp(d/K)$ is qf-internal to the set of $\mathrm{Aut}(\mathcal{U}/K)$-conjugates of $tp(a/K(c)_{\sigma^{\pm 1}})$, and is therefore π-analysable.

If d' is a field conjugate of d over L, then d' realises $qftp(d/L)[\ell]$ for some $\ell \geq 1$. As b belongs to the field generated over K by field conjugates of d over L, i.e., by realisations of $qftp(d/L)[\ell]$ for some ℓ (see the remark at the end of 2.3), Proposition 2.16 implies that $tp(b/K)$ is π-analysable. $\square$

3 Descent

Proposition 3.1. *Let $(\mathcal{U},\sigma)$ be a difference field, and $K_1 \subset K_2$ be subfields of the fixed field* $\mathrm{Fix}(\sigma)$ *of $\mathcal{U}$, with K_2/K_1 regular and $SU(a/K_2) < \infty$. Let a, b be tuples in $\mathcal{U}$ such that:*

(a) *$a \in K_2(b)_{\sigma^{\pm 1}}$;*

(b) *$K_1(b)_{\sigma^{\pm 1}}$ is linearly disjoint from K_2 over K_1;*

(c) *$tp(a/K_2)$ is hereditarily orthogonal to* $\mathrm{Fix}(\sigma)$.

Then there is a tuple c in $K_1(b)^{\mathrm{perf}}_{\sigma^{\pm 1}} \cap K_2(a)^{\mathrm{perf}}_{\sigma^{\pm 1}}$ such that $a \in K_2(c)_{\sigma^{\pm 1}}$. If $tr.deg(K_2(a)_\sigma/K_2) = 1$ and K_1 is perfect, or if the characteristic is 0, then $K_1(b)_{\sigma^{\pm 1}} \cap K_2(a)_{\sigma^{\pm 1}} = K_2(c)_{\sigma^{\pm 1}}$.

Proof. We may assume $(\mathcal{U},\sigma)$ is existentially closed and saturated. Let e be a finite tuple in K_2 be such that $a \in K_1(e,b)_{\sigma^{\pm 1}}$, and $K_1(e,a)_{\sigma^{\pm 1}}$ and K_2 are linearly disjoint over $K_1(e)_{\sigma^{\pm 1}}$. Let $K_1(d)_{\sigma^{\pm 1}} = \text{qf-Cb}_{K_1}(e, a/K_1(b)_{\sigma^{\pm 1}})$.

As K_2/K_1 is separable (and $b \downarrow_{K_1} K_2$, $e \in K_2$), so is the extension $K_1(b,e,a)_{\sigma^{\pm 1}} = K_1(b,e)_{\sigma^{\pm 1}}$ of $K_1(b)_{\sigma^{\pm 1}}$; hence $d \in K_1(b)_{\sigma^{\pm 1}}$. From the linear disjointness of $K_1(b)_{\sigma^{\pm 1}}$ and $K_1(a,d,e)_{\sigma^{\pm 1}}$ over $K_1(d)_{\sigma^{\pm 1}}$ and the fact that $a \in K_1(b,e)_{\sigma^{\pm 1}}$, we obtain $a \in K_1(d,e)_{\sigma^{\pm 1}}$. Since $e \downarrow_{K_1} b$, by Theorem 2.17, $tp(d/K_1)$ is hereditarily orthogonal to $\mathrm{Fix}(\sigma)$.

Let $K_1(c)_{\sigma^{\pm 1}} = \text{qf-Cb}_{K_1}(d/K_1(e,a)_{\sigma^{\pm 1}})$; by Theorem 2.17, $tp(c/K_1)$ is hereditarily orthogonal to $\mathrm{Fix}(\sigma)$, which implies $c \downarrow_{K_1} e$ (since $e \in K_2 \subset \mathrm{Fix}(\sigma)$). By definition of c, the fields $K_1(c,d)_{\sigma^{\pm 1}}$ and $K_1(e,a)^{\mathrm{perf}}_{\sigma^{\pm 1}}$ are linearly disjoint over $K_1(c)_{\sigma^{\pm 1}}$; as $a \in K_1(e,d)_{\sigma^{\pm 1}}$, this implies that $a \in K_1(c,e)_{\sigma^{\pm 1}}$, and therefore $K_2(a)^{\mathrm{perf}}_{\sigma^{\pm 1}} = K_2(c)^{\mathrm{perf}}_{\sigma^{\pm 1}}$.

For the first assertion, it remains to show that c can be taken in $K_1(b)^{\mathrm{perf}}_{\sigma^{\pm 1}}$.

We now use that K_2 is a regular extension of K_1. We know that $c \in K_2(a)^{\mathrm{perf}}_{\sigma^{\pm 1}} \subset K_2(b)^{\mathrm{perf}}_{\sigma^{\pm 1}}$; we also know that $tp(c/K_1)$ is hereditarily orthogonal to $\mathrm{Fix}(\sigma)$; as $b \downarrow_{K_1} K_2$ and $c \in \mathrm{acl}(K_2 b)$, this implies $c \in \mathrm{acl}(K_1 b)$. The regularity of K_2/K_1 then implies that K_2^{perf} and $K_1(b,c)^{\mathrm{perf}}_{\sigma^{\pm 1}}$ are linearly disjoint over K_1^{perf}, and gives $c \in K_1(b)^{\mathrm{perf}}_{\sigma^{\pm 1}}$.

Note that if the characteristic is 0, then we directly obtain that $K_1(c)_{\sigma^{\pm 1}} = K_1(b)_{\sigma^{\pm 1}} \cap K_2(a)_{\sigma^{\pm 1}}$. Assume that the characteristic is positive, that K_1 is perfect and that $tr.deg(K_2(a)_{\sigma^{\pm 1}}/K_2) = 1$. Then $tr.deg(K_1(c)_{\sigma^{\pm 1}}/K) = 1$ and we can apply Lemma 2.6, as for some n, we have $c^{p^n} \in K_2(a)_{\sigma^{\pm 1}}$: if c' is such that $K_1(c)_{\sigma^{\pm 1}} \cap K_2(a)_{\sigma^{\pm 1}} = K_1(c')_{\sigma^{\pm 1}}$, then $K_2(c')_{\sigma^{\pm 1}} = K_2(a)_{\sigma^{\pm 1}}$.

Theorem 3.2. *Let $(\mathcal{U},\sigma)$ be a difference field, and $K_1 \subset K_2$ be subfields of the fixed field* $\mathrm{Fix}(\sigma)$ *of $\mathcal{U}$, with K_2/K_1 regular. Let a, b be tuples in $\mathcal{U}$ such that $SU(a/K_2) < \infty$ and:*

(a) *$a \in K_2(b)_\sigma$;*

(b) *$K_1(b)_\sigma$ is linearly disjoint from K_2 over K_1;*

(c) *$tp(a/K_2)$ is hereditarily orthogonal to* $\mathrm{Fix}(\sigma)$.

Then there is a tuple c in $K_1(b)_\sigma^{\rm perf}$ such that $a \in K_2(c)_\sigma$ and c is purely inseparable over $K_2(a)_\sigma$. If $tr.deg(K_2(a)_\sigma/K_2) = 1$ and K_1 is perfect, then one can choose c so that $K_1(b)_\sigma \cap K_2(a)_\sigma = K_1(c)_\sigma$.

Proof. Let c be given by Proposition 3.1; we may choose it such that $K_1(c)_{\sigma^{\pm 1}} \subseteq K_1(c)_\sigma^{alg}$ and $a \in K_2(c)_\sigma$ (replace c by $(\sigma^{-m}(c), \dots, \sigma^{-n}(c))$ for some $n \leq m$). Choose $i \geq 0$ such that $\sigma^i(c) \in K_1(b)_\sigma^{\rm perf} \cap K_2(a)_\sigma^{\rm perf}$.

Choose a tuple d such that $K_1(d)_\sigma = K_1(c)_\sigma \cap K_1(\sigma^i(c))_\sigma^{sep}$. Then $a \in K_2\,{\rm acl}(K_1 d)$. Also, we know that $\sigma^i(a) \in K_2(d)_\sigma$, and this implies that $K_2(d,a)_\sigma$ is a finite extension of $K_2(d)_\sigma$, which is contained in $K_2(c)_\sigma$. As K_2/K_1 is regular, $(K_1(b)_\sigma)^{alg}$ and K_2 are linearly disjoint over K_1; by Lemma 2.6(a), this gives $K_2(d,a)_\sigma \cap K_2(d)_\sigma^{sep} = K_2(d)_\sigma$, and therefore $a \in K_2(d)_\sigma^{\rm perf}$. Replacing d by $d^{p^{-m}}$ for some m, we have $a \in K_2(d)_\sigma$. This gives us the general case.

Assume now that K_1 is perfect and $tr.deg(K_2(a)_\sigma/K_2) = 1$; then also $tr.deg(K_1(c)_\sigma/K_1) = 1$. We reason as before: the element c can now be chosen in $K_2(a)_{\sigma^{\pm 1}} \cap K_1(b)_{\sigma^{\pm 1}}$, and such that $a \in K_2(c)_\sigma$, and for some i, $\sigma^i(c) \in K_2(a)_\sigma$. Then $K_2(a)_\sigma$ is a field between $K_2(c)_\sigma$ and $K_2(\sigma^i(c))_\sigma$, and Lemma 2.6 now gives us a tuple d such that $K_1(d)_\sigma = K_2(a)_\sigma \cap K_1(c)_\sigma$, and $K_2(a)_\sigma = K_2(d)_\sigma$.

Theorem 3.3. *Let $K_1 \subset K_2$ be fields, with K_2/K_1 regular, V_2 an irreducible variety over K_2, and $(V_2, \phi_2) \in AD_{K_2}$. Assume that (V_2, ϕ_2) is primitive and $\deg(\phi_2) > 1$. Assume furthermore that for some $n \geq 1$, (V_2, ϕ_2^n) is dominated (in AD_{K_2}) by some object of AD_{K_1}.*

(1) *There is some variety V_3 defined over K_1, and a dominant constructible map $\phi_3 : V_3 \to V_3$ also defined over K_1, a constructible isomorphism $h : (V_2, \phi_2) \to (V_3, \phi_3)$.*

(2) *Assume that the characteristic is 0, or that K_1 is perfect and $\dim(V_2) = 1$. Then (V_2, ϕ_2) is rationally isotrivial, i.e., there is some $(V_3, \phi_3) \in AD_{K_1}$ which is isomorphic to (V_2, ϕ_2) (in AD_{K_2}).*

Proof. Let $(V_1, \phi_1) \in AD_{K_1}$ dominate (V_2, ϕ_2^n), via a map f. The map ϕ_1 permutes the absolutely irreducible components of V_1, and for some m, ϕ_1^m leaves them invariant.

Let $\mathcal{U}$ be a saturated, existentially closed difference field containing K_2 and such that σ is the identity on K_2^{alg}. By saturation of $\mathcal{U}$, there is a generic b of V_1 over K_2 which satisfies $\sigma(b) = \phi_1^m(b)$. By assumption, $f(b) = a$ is a generic of V_2 and satisfies $\sigma(a) = \phi_2^{mn}(a)$.

Claim. $tp(a/K_2)$ is hereditarily orthogonal to ${\rm Fix}(\sigma)$.

By primitivity and Proposition 2.14, if the claim is false then $tp(a/K_2)$ is almost internal to ${\rm Fix}(\sigma)$. By Lemma 1.11(4), we have $ild(a/K_2) = ld(a/K_2) = 1$, which contradicts the assumption.

By Theorem 3.2, there is $c \in K_1(b)^{\rm perf} \cap K_2(a)^{\rm perf}$ such that $a \in K_2(c)$. Thus there is a constructible isomorphism $g : V_2 \to V_3$, where V_3 is the algebraic locus of c over K_1, and such that $g(a) = c$. Consider now $a' = \phi_2(a)$, and $c' = g(a')$. Then $\sigma(a') = \phi_2^{mn+1}(a) = \phi_2^{mn}(a')$, and, because V_2 was K_2-irreducible, we have

$$qftp(a/K_2) = qftp(a'/K_2), \qquad qftp(c/K_2) = qftp(c'/K_2).$$

As $tp(c/K_2)$ is hereditarily orthogonal to $\mathrm{Fix}(\sigma)$ (i.e., to $tp(K_2/K_1)$) and $c \downarrow_{K_1} K_2$, it follows (by 2.17) that $cc' \downarrow_{K_1} K_2$. As K_2/K_1 is regular, the fields $K_1(c,c')$ and K_2 are linearly disjoint over K_1, and this implies that $c' \in K_1(c)^{\mathrm{perf}}$ (recall that $c' \in K_2(c)^{\mathrm{perf}}$). Hence, for some dominant constructible $\phi_3 : V_3 \to V_3$ sending c to c', we have $g : (V_2, \phi_2) \simeq (V_3, \phi_3)$. This shows (2).

Assume now that K_1 is perfect, and $\dim(V_2) = 1$. Using Theorem 3.2, we get c such that $K_1(b) \cap K_2(a) = K_1(c)$ and $K_2(c) = K_2(a)$, whence a birational isomorphism $g : V_2 \to V_3$. Defining $a' = \phi_2(a)$ and $c' = g(a')$, we obtain $c' \in K_2(c) \cap K_1(c)^{alg} = K_1(c)$, i.e., if $\phi_3 = g\phi_2 g^{-1}$, then ϕ_3 is a dominant morphism defined over K_1, and $g : (V_2, \phi_2) \simeq (V_3, \phi_3)$. ☐

Remarks 3.4. (1) The proof of Theorem 3.3 actually shows more: in the above notation, the fact that $c \in K_1(b)_\sigma^{\mathrm{perf}}$ means that the composed constructible morphism $g \circ f : V_1 \to V_2 \to V_3$ is defined over K_1^{perf}.

(2) The hypothesis on the degree of ϕ can be replaced by (V, ϕ) fixed-field-free.

(3) Inspection of the proof of Proposition 3.1 shows that the hypotheses that

$K_1 \subset K_2 \subset \mathrm{Fix}(\sigma)$ *and* $tp(a/K_2)$ *is hereditarily orthogonal to* $\mathrm{Fix}(\sigma)$

can be be changed to:

K_2/K_1 *is regular, and* $tp(K_2/K_1)$ *is hereditarily orthogonal to all types occurring in a semi-minimal analysis of* $tp(a/K_2)$.

(4) Also, as observed (and proved) in 1.9 of [4], to obtain isogeny isotriviality, the only assumption needed on $K_1 \subset K_2$ and a is that $tp(a/K_2)$ is one-based.

(5) Theorem 3.3, together with Lemma 3.4 and Remark 3.5(2h) in [4], gives the result of M. Baker, Theorem 1.6 in [1].

3.5. Example. *An algebraic dynamics over $k(t)$, dominated by an algebraic dynamics over k, but not isogenous to a difference variety over k.*

Let H be a vector extension of an Abelian variety; i.e. there exists an exact sequence of algebraic groups $0 \to V \to H \to A \to 0$ with A an Abelian variety, $V \cong \mathbb{G}_a^n$ a vector group. Assume $\dim(V) = 2$ and $\mathrm{Hom}(H, \mathbb{G}_a) = (0)$. Assume H is defined over k, and identify the projective space $\mathbb{P}V$ with $\mathbb{P}^1$. In particular a transcendental element t gives a one-dimensional subspace V_t of V. Let $H_t = H/V_t$. Fix $h \in H$ generating H; it suffices that the image of h in A generate A; if A is a simple Abelian variety, it suffices therefore that the image is non-torsion. Let $Y = (H, T(h))$ and $X_t = (H_t, T(h_t))$ where h_t is the image of h in H_t, and $T(g)$ denotes translation by g. Then Y dominates X_t. But X_t is clearly not isotrivial.

References

[1] M. Baker, A finiteness theorem for canonical heights attached to rational maps over function fields, available at `arXiv:math.NT/0601046`.

[2] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, Trans. Amer. Math. Soc. 351 (1999), pp. 2997-3071.

[3] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics, Proc. London Math. Soc. (3) 85 (2002) 257 – 311.

[4] Z. Chatzidakis, E. Hrushovski, Difference fields and descent in algebraic dynamics, I, this volume.

[5] Z. Chatzidakis, E. Hrushovski, Difference fields and descent in algebraic dynamics, III, in preparation.

[6] R.M. Cohn, *Difference algebra*, Tracts in Mathematics 17, Interscience Pub. 1965.

[7] Ehud Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, Annals of Pure and Applied Logic, vol. 112 (2001), no. 1, pp. 43 – 115.

[8] F. Wagner, Some remarks on one-basedness, J. of Symb. Logic 69 Nr 1 (2004), 34 – 38.

Current addresses:

UFR de Mathématiques
Université Paris 7 - Case 7012
2, place Jussieu
75251 Paris Cedex 05
France
e-mail: `zoe@logique.jussieu.fr`

Institute of Mathematics
The Hebrew University
Givat Ram
91904 Jerusalem
Israel
e-mail: `ehud@math.huji.ac.il`